PCT/EP 99/03385

BUNDESREPUBLIK DEUTSCHLAND

EP99/3385

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

REC'D 20 JUL 1999
WIPO PCT

Bescheinigung

Die Giesecke & Devrient GmbH in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Zugriffsgeschützter Datenträger"

am 18. Mai 1998 beim Deutschen Patent- und Markenamt eingereicht.

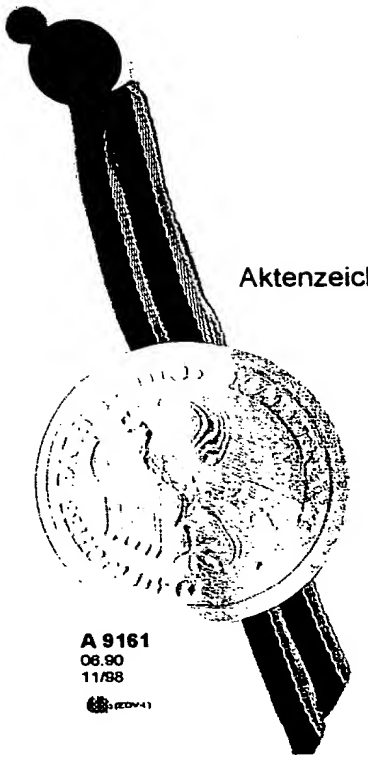
Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 06 K 19/073 der Internationalen Patentklassifikation erhalten.

München, den 14. Juni 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Agurks

Aktenzeichen: 198 22 218.1



A 9161
06.90
11/98

Zugriffsgeschützter Datenträger

Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind. Insbesondere betrifft die Erfindung eine Chipkarte.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren

oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikrosonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z.B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

Der Erfindung liegt die Aufgabe zugrunde, geheime Daten, die in dem Chip eines Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen.

Diese Aufgabe wird durch die Merkmalskombination des Anspruchs 1 gelöst.

Bei der erfindungsgemäßen Lösung werden im Gegensatz zum Stand der Technik keine Maßnahmen getroffen, um ein Freilegen der internen Strukturen des Chips und ein Anbringen von Mikrosonden zu verhindern. Es werden stattdessen Maßnahmen getroffen, die es einem potientellen Angreifer erschweren, aus den gegebenenfalls abgehörten Signalverläufen Rückschlüsse auf geheime Informationen zu schließen. Die Signalverläufe hängen von den Operationen ab, die der Chip gerade ausführt. Wenn diese Operationen immer nach demselben starren Schema ausgeführt werden, d.h. insbesondere immer in derselben Reihenfolge und der Angreifer diese Reihenfolge kennt, muß ein Angreifer weit weniger Schwierigkeiten überwinden, um Daten auszuspähen als wenn er noch nicht einmal weiß, welche Operation zu welchem Zeitpunkt gerade abgearbeitet wird. Es ist daher gemäß der Erfindung vorgesehen, bei der Abarbeitung von sicherheitsrelevanten Operationen innerhalb der Chipkarte sich möglichst weit von einem starren Ab-

laufschema zu entfernen und dem Angreifer dadurch möglichst keine Ansatzpunkte für eine Analyse der geheimen Daten zu bieten. Dies wird dadurch erreicht, daß möglichst viele, im Idealfall sogar alle Operationen, die insofern voneinander unabhängig sind, daß jede der Operationen keine Daten benötigt, die von den anderen Operationen ermittelt werden, in einer variablen, beispielsweise zufallsbedingten oder von Eingangsdaten abhängigen Reihenfolge abgearbeitet werden. Dadurch wird erreicht, daß ein Angreifer, der sich in der Regel an der Reihenfolge der Operationen orientieren wird, nicht ohne weiteres herausfinden kann, welche Operation gerade abgearbeitet wird. Dies gilt in besonderem Maße dann, wenn sich die Operationen bezüglich des von ihnen bei gleichen Eingangsdaten hervorgerufenen Signalverlaufs sehr stark ähneln oder sogar gleich sind. Wenn dem Angreifer aber nicht einmal die Art der Operation bekannt ist, die gerade abgearbeitet wird, ist es extrem schwierig, gezielt Daten auszuspähen. Wenn die Gefahr besteht, daß ein Angreifer sehr viele Ausspähversuche unternehmen wird, um die zufallsbedingte Variation der Reihenfolge herauszumitteln, empfiehlt es sich, die Variation von den Eingangsdaten abhängig zu machen.

Die Erfindung wird nachstehend anhand der in den Figuren dargestellten Ausführungsformen erläutert. Es zeigen:

Fig. 1 eine Chipkarte in Aufsicht,

Fig. 2 einen stark vergrößerten Ausschnitt des Chips der in Fig. 1 dargestellen Chipkarte in Aufsicht und

Fig. 3 eine schematische Darstellung der Abfolge bei der Abarbeitung einiger Operationen durch die Chipkarte.

In Fig. 1 ist als ein Beispiel für den Datenträger eine Chipkarte 1 dargestellt. Die Chipkarte 1 setzt sich aus einem Kartenkörper 2 und einem Chipmodul 3 zusammen, das in eine dafür vorgesehene Aussparung des Kartenkörpers 2 eingelassen ist. Wesentliche Bestandteile des Chipmoduls 3 sind Kontaktflächen 4, über die eine elektrische Verbindung zu einem externen Gerät hergestellt werden kann und ein Chip 5, der mit den Kontaktflächen 4 elektrisch verbunden ist. Alternativ oder zusätzlich zu den Kontaktflächen 4 kann auch eine in Fig. 1 nicht dargestellte Spule oder ein anderes Übertragungmittel zur Herstellung einer Kommunikationsverbindung zwischen dem Chip 5 und einem externen Gerät vorhanden sein.

In Fig. 2 ist ein stark vergrößerter Ausschnitt des Chips 5 aus Fig. 1 in Aufsicht dargestellt. Das besondere der Fig. 2 liegt darin, daß die aktive Oberfläche des Chips 5 dargestellt ist, d.h. sämtliche Schichten, die im allgemeinen die aktive Schicht des Chips 5 schützen, sind in Fig. 2 nicht dargestellt. Um Informationen über die Signalverläufe im Inneren des Chips zu erhalten, können beispielsweise die freigelegten Strukturen 6 mit Mikrosonden kontaktiert werden. Bei den Mikrosonden handelt es sich um sehr dünne Nadeln, die mittels einer Präzisions-Positioniereinrichtung mit den freigelegten Strukturen 6, beispielsweise Leiterbahnen in elektrischen Kontakt gebracht werden. Die mit den Mikrosonden aufgenommenen Signalverläufe werden mit geeigneten Meß- und Auswerteeinrichtungen weiterverarbeitet mit dem Ziel, Rückschlüsse auf geheime Daten des Chips schließen zu können.

Mit der Erfindung wird erreicht, daß ein Angreifer auch dann, wenn es ihm gelungen sein sollte, die Schutzschicht des Chips 5 ohne Zerstörung des Schaltkreises zu entfernen und die freigelegten Strukturen 6 des Chips 5 mit Mikrosonden zu kontaktieren oder auf andere Weise abzuhören nur sehr schwer oder gar nicht Zugang zu insbesondere geheimen Daten des Chips

erlangt. Selbstverständlich greift die Erfindung auch dann, wenn ein Angreifer auf andere Art und Weise Zugang zu den Signalverläufen des Chips 5 erlangt.

Fig. 3 zeigt eine schematische Darstellung der Abfolge bei der Abarbeitung einiger Operationen durch die Chipkarte. In Fig. 3 ist insbesondere dargestellt, welche Operationen von der Chipkarte 1 zwingend sequentiell abgearbeitet werden müssen, da sie voneinander abhängen und welche Operationen im Prinzip parallel und damit auch in einer beliebigen Reihenfolge abgearbeitet werden können. Hierzu ist in Fig. 3 ein Ausschnitt aus einem Programmdurchlauf der Chipkarte 1 dargestellt, in dem Daten abc verarbeitet werden. Alle zwingend sequentiell abzuarbeitenden Operationen sind in Fig. 3 sequentiell aufeinanderfolgend dargestellt. Alle Operationen bei denen es nicht auf die Reihenfolge der Abarbeitung untereinander ankommt, sind parallel zueinander angeordnet.

Die Bearbeitung der Daten abc beginnt mit einer Operation P1, die in Form eines Blockes 7 dargestellt ist. An dem Block schließt sich sequentiell ein Block 8 an, der die Operation P2 repräsentiert. Aus Fig. 3 ergibt sich somit, daß die Bearbeitungsreihenfolge der Operationen P1 und P2 nicht vertauscht werden kann, d.h. zwingend fest ist. Nach Block 8 verzweigt sich das in Fig. 3 dargestellte Schema zu fünf Blöcken 9, 10, 11, 12, 13, die die Operationen P3, P4, P5, P6 und P7 repräsentieren. Daraus ergibt sich, daß die Blöcke P3, P4, P5, P6 und P7 gleichzeitig abgearbeitet werden können und somit auch in einer beliebigen Reihenfolge abgearbeitet werden können. Erfindungsgemäß wird die Reihenfolge der Abarbeitung dieser Operationen P3, P4, P5, P6, P7 bei jedem Durchlauf variiert, d.h. es ist für einen Angreifer nicht absehbar, welche dieser Operationen sich an die Operation P2 anschließt, welche Operationen wiederum danach durchgeführt wird usw. Die Variation

der Reihenfolge kann entweder nach einem fest vorgegebenen Schema oder besser noch zufallsbedingt oder abhängig von Eingangsdaten erfolgen, indem mittels einer Zufallszahl bzw. durch die Eingangsdaten jeweils festgelegt wird, welche der Operationen P3, P4, P5, P6 und P7 als nächste abgearbeitet wird. Durch diese gegebenenfalls zufallsbedingte Variation der Abarbeitung der einzelnen Operationen wird ein Ausspähen der mit den Operationen verarbeiteten Daten erschwert. Wenn alle Operationen P3, P4, P5, P6 und P7 abgearbeitet sind, schließt sich zwingend die Operation P8 an, deren Bearbeitungsreihenfolge nicht variabel ist. Die Operation P8 ist durch den Block 14 dargestellt. Auf die Operation P8 können weitere, und zwar sowohl in der Reihenfolge variable als auch in der Reihenfolge feste Operationen folgen, die allerdings in der Fig. 3 nicht mehr dargestellt sind.

Die Erfindung kann beispielsweise im Rahmen der Abarbeitung von Verschlüsselungsalgorithmen eingesetzt werden, die häufig ähnliche Operationen enthalten, deren Bearbeitungsreihenfolge variierbar ist. Die Bearbeitungsreihenfolge kann dabei entweder jeweils vor der ersten variierbaren Operation gemeinsam für alle mit dieser ersten Operation vertauschbaren Operationen festgelegt werden oder es kann auch vor jeder variierbaren Operation aus der Menge der noch verbleibenden variierbaren Operationen die nächste zu bearbeitende Operation bestimmt werden. In beiden Fällen können zur Festlegung der Bearbeitungsreihenfolge Zufallszahlen herangezogen werden.

Patentansprüche

1. Datenträger mit einem Halbleiterchip (5), der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, mit dem eine Vielzahl von Operationen ausgeführt werden kann, wobei für wenigstens eine Untermenge dieser Operationen gilt, daß das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen abhängt, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

2. Datenträger nach Anspruch 1, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung bei jedem Durchlauf durch die genannte Untermenge der Operationen variiert wird.

3. Datenträger nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung nach einem fest vorgegebenen Prinzip variiert wird.

4. Datenträger nach einem der Anprüche 1 bis 3, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung zufallsbedingt variiert wird.

5. Datenträger nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung abhängig von den mit den Operationen verarbeiteten Daten variiert wird.

6. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung jeweils vor der Ausführung der ersten Operation der Untermenge für alle Operationen der Untermenge festgelegt wird, deren Ausführung unmittelbar aufeinanderfolgend vorgesehen ist.

7. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß jeweils vor Beginn der Ausführung einer Operation der Untermenge festgelegt wird, welche der Operationen der Untermenge, deren Ausführung aufeinanderfolgend vorgesehen ist, als nächste ausgeführt wird.

8. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei dem Datenträger um eine Chipkarte handelt.

Zusammenfassung

Die Erfindung betrifft einen Datenträger (1), der einen Halbleiterchip (5) aufweist. Um zu verhindern, daß ein Angreifer aus abgehörten Signalverläufen des Chips (5) geheime Daten des Chips (5) ermittelt, werden zumindest bei sicherheitsrelevanten Operationen möglichst viele Einzeloperationen, bei deren Ausführung es nicht auf die Reihenfolge ankommt, in einer variablen Reihenfolge ausgeführt. Die Reihenfolge der Ausführung kann dabei fest vorgegeben sein, nach dem Zufallsprinzip variiert werden oder von den mit den Operationen verarbeiteten Daten abhängen.

(Fig. 1)

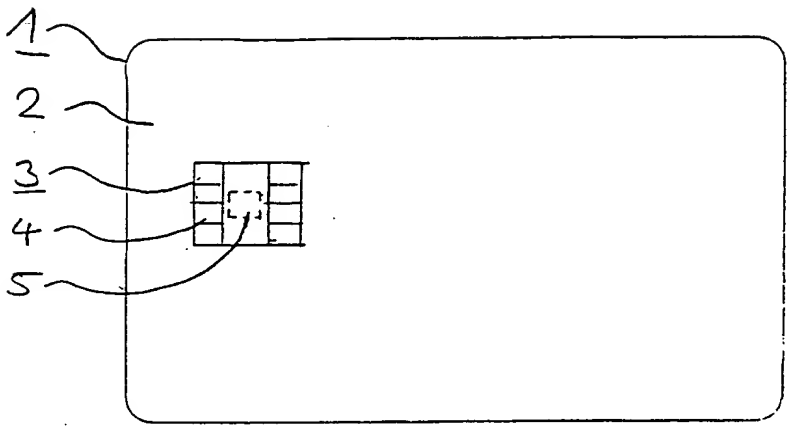


Fig. 1

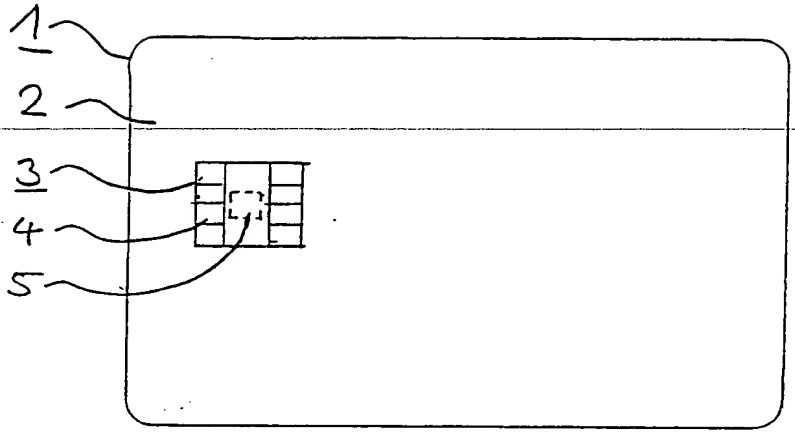


Fig. 1

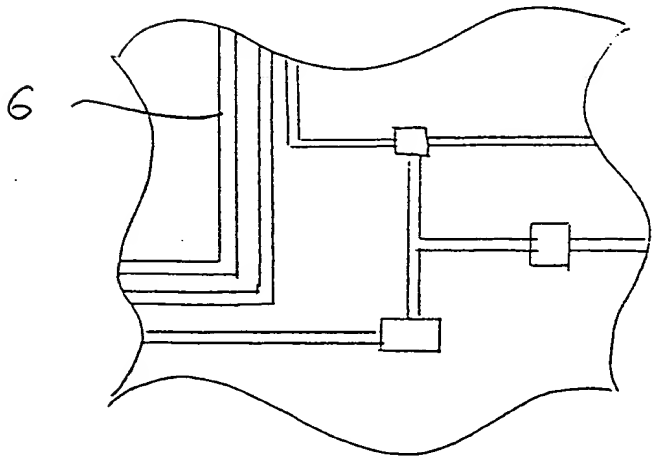


Fig. 2

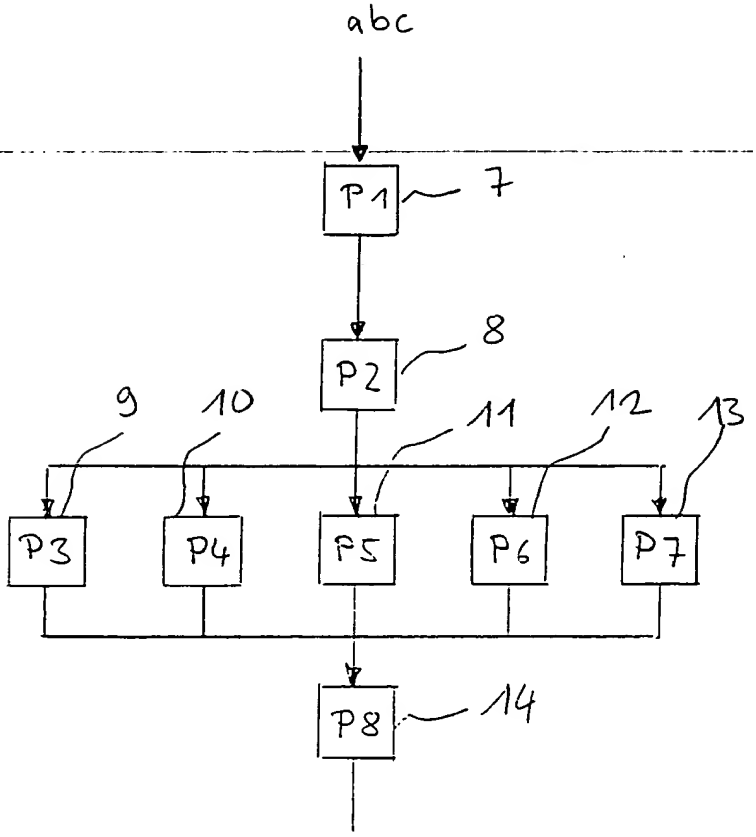


Fig. 3